(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-45756
(P2005-45756A)
(43)公開日　平成17年2月17日(2005.2.17)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601C	5B017
G06F	12/14	G06F	12/14	320E	5B085
G06F	15/00	G06F	15/00	330Z	5D044
G09C	1/00	G09C	1/00	640E	5J104
G11B	20/10	G11B	20/10	D	

審査請求 未請求　請求項の数 31　OL　（全 28 頁）　最終頁に続く

(21)出願番号　特願2003-406359(P2003-406359)
(22)出願日　平成15年12月4日(2003.12.4)
(31)優先権主張番号　特願2003-194491(P2003-194491)
(32)優先日　平成15年7月9日(2003.7.9)
(33)優先権主張国　日本国(JP)

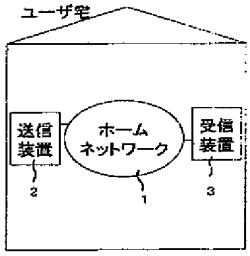
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100075812
弁理士　吉武　賢次
(74)代理人　100088889
弁理士　橘谷　英俊
(74)代理人　100082991
弁理士　佐藤　泰和
(74)代理人　100096921
弁理士　吉元　弘
(74)代理人　100103263
弁理士　川崎　康

最終頁に続く

(54)【発明の名称】情報通信装置、通信システム及びデータ伝送制御プログラム

(57)【要約】
【課題】　著作権保護を図りつつ、著作権保護の必要な電子データを有効利用できるようにする。
【解決手段】　本発明に係る通信システムは、個人宅内で主にAVデータを送受信することを目的としており、ホームネットワーク１に接続された送信装置２及び受信装置３を備えている。デバイスIDの登録要求を行ってから所定時間以内に応答が返ってきた場合のみ、他の通信装置（受信装置３または送信装置２）の登録を行うようにしたため、有限の範囲内の通信装置との間でのみAVデータの伝送を行うことができ、簡易な処理でAVデータの著作権保護を図ることができる。
【選択図】　図１

第1の実施形態の概略構成



【特許請求の範囲】
【請求項１】
他の通信装置との間で、著作権保護のための暗号化された電子データを伝送する情報通信装置において、
ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、
前記他の通信装置が予め定めた距離的な条件を満たす場合、または前記他の通信装置と共通の識別情報を携帯装置から受信した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、
前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。
【請求項２】
他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、
ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、
前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、
前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。
【請求項３】
他の通信装置から送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、
ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、
前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、
前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。
【請求項４】
ローカルネットワークに接続されたインターフェース手段を備え、
前記事前登録手段は、前記他の通信装置が前記ローカルネットワークに直接接続されている場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録することを特徴とする請求項２または３に記載の情報通信装置。
【請求項５】
前記他の通信装置に対して装置識別情報の送信要求を行ってから、該他の通信装置からの装置識別情報が受信されるまでの時間が予め定めた時間以内か否かを判断する応答時間判断手段を備え、
前記事前登録手段は、前記応答時間判断手段により前記時間以内と判断された場合に、前記他の通信装置の装置識別情報を登録することを特徴とする請求項２乃至４のいずれかに記載の情報通信装置。
【請求項６】
前記識別情報管理手段に登録された装置識別情報の数が予め定めた上限数に達した場合には、前記事前登録手段は、それ以上の装置識別情報の登録を拒絶するか、もしくは最も古くに登録された装置識別情報と最も長い間通信を行っていない他の通信装置の装置識別

情報との少なくとも一方を削除した上で、新たな装置識別情報を登録することを特徴とする請求項２乃至５のいずれかに記載の情報通信装置。

【請求項７】

前記他の通信装置からの認証・鍵交換要求を受信する認証・鍵交換要求受信手段を備え、

前記事前登録手段は、前記認証・鍵交換要求受信手段で認証・鍵交換要求が受信された後に、前記他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行うことを特徴とする請求項２乃至６のいずれかに記載の情報通信装置。

【請求項８】

前記事前登録手段は、前記他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を、データリンクレイヤフレームまたは物理レイヤフレームにて行うことを特徴とする請求項２乃至７のいずれかに記載の情報通信装置。

【請求項９】

前記認証・鍵交換処理手段による認証鍵交換に成功した場合に、前記他の通信装置との間で前記電子データをやり取りする制御を行うデータ伝送処理手段を備え、

前記認証・鍵交換処理手段及び前記データ伝送処理手段は、IP（Internet Protocol）パケットを用いて各処理を行うことを特徴とする請求項２乃至８のいずれかに記載の情報通信装置。

【請求項１０】

送信装置と、

前記送信装置から送信された、著作権保護のための暗号化を行った電子データを受信する受信装置と、を備える通信システムにおいて、

前記送信装置及び前記受信装置の少なくとも一方は、

ネットワークを介して取得した他方の装置の装置識別情報を登録する識別情報管理手段と、

前記他方の装置が所定の有限範囲内のネットワークに接続されていると認識できる場合に、該他方の装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、

前記識別情報管理手段に登録されている装置識別情報を持つ前記他方の装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする通信システム。

【請求項１１】

送信装置と、前記送信装置から送信された著作権保護のための暗号化を行った電子データを受信する受信装置と、の間で、電子データを伝送する制御を行うデータ伝送制御プログラムにおいて、

ネットワークを介して取得した前記他の通信装置の装置識別情報を登録するステップと、

前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識できる場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行うステップと、

前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を実行させるための伝送制御プログラム。

【請求項１２】

ネットワークを介して他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、

識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、

受信された前記固有の識別情報を登録する識別情報登録手段と、

前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録

判断手段と、
前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第１の認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。
【請求項１３】
他の通信装置からネットワークを介して送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、
識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、
受信された前記固有の識別情報を登録する識別情報登録手段と、
前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、
前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第１の認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。
【請求項１４】
前記暗号化された電子データを受信する入力処理手段と、
前記入力処理手段で受信された電子データを、復号した後に出力する出力処理手段と、を備えることを特徴とする請求項１３に記載の情報通信装置。
【請求項１５】
前記固有の識別情報の登録開始を指示する登録開始指示手段をさらに備え、
前記識別情報登録手段は、前記登録開始指示手段による指示があった場合に、登録処理を行うことを特徴とする請求項１２乃至１４のいずれかに記載の情報通信装置。
【請求項１６】
前記登録開始指示手段による指示があった場合に前記通信手段に電源電圧を供給する電源制御手段をさらに備えることを特徴とする請求項１５に記載の情報通信装置。
【請求項１７】
前記通信手段を介して、前記識別情報送信装置との間で認証鍵交換を行う第２の認証鍵交換処理手段をさらに備え、
前記識別情報登録手段は、前記第２の認証鍵交換処理手段による認証鍵交換に成功した場合に、登録処理を行うことを特徴とする請求項１２乃至１６のいずれかに記載の情報通信装置。
【請求項１８】
前記識別情報送信装置に対して特定のパケットを送信し、これに対する前記識別情報送信装置からの応答パケットが返ってくるまでのラウンドトリップ時間を計測する計測手段を備え、
前記第２の認証鍵交換処理手段は、前記計測手段で計測されたラウンドトリップ時間が所定時間以下の場合に認証鍵交換を行うことを特徴とする請求項１７に記載の情報通信装置。
【請求項１９】
前記計測手段によるラウンドトリップ時間の計測が終了した後に、前記識別情報登録手段による処理を開始することを特徴とする請求項１８に記載の情報通信装置。
【請求項２０】
前記識別情報登録手段が前記固有の識別情報を登録した旨を通知する登録通知手段をさらに備えることを特徴とする請求項１２～１９のいずれかに記載の情報通信装置。
【請求項２１】
前記通信手段で受信された前記固有の識別情報を暗号化する暗号化手段と、
前記暗号化手段で暗号化された前記固有の識別情報を前記識別情報登録手段に伝送する暗号化情報伝送手段と、をさらに備えることを特徴とする請求項１２乃至２０のいずれかに記載の情報通信装置。

【請求項２２】
前記固有の識別情報は、個々の前記識別情報送信装置に固有のものであることを特徴とする請求項１２乃至２１のいずれかに記載の情報通信装置。
【請求項２３】
前記識別情報登録手段は、互いに異なる前記固有の識別情報の登録数を、予め定めた所定数以下に制限することを特徴とする請求項１２乃至２２のいずれかに記載の情報通信装置。
【請求項２４】
ネットワークを介して著作権保護のための暗号化された電子データを伝送する第１及び第２の通信装置に対して、識別情報を送信する情報通信装置であって、
前記第１及び第２の通信装置が前記電子データを伝送するのに必要な固有の識別情報を保持する識別情報保持手段と、
前記第１及び第２の通信装置に対して前記固有の識別情報を送信する通信手段と、を備えることを特徴とする情報通信装置。
【請求項２５】
前記識別情報保持手段は、保持可能な識別情報の数を所定個に制限することを特徴とする請求項２４に記載の情報通信装置。
【請求項２６】
前記通信手段は、赤外線を用いて前記第１及び第２の通信装置の間で無線通信を行うことを特徴とする請求項２４または２５に記載の情報通信装置。
【請求項２７】
前記通信手段は、双方向の赤外線通信手段であり、
前記通信手段とは別個に、片方向の赤外線通信を行う片方向通信手段をさらに備えることを特徴とする請求項２６に記載の情報通信装置。
【請求項２８】
前記通信手段は、受信電波により生成された電力を利用して前記第１及び第２の通信装置の間で無線通信を行うことを特徴とする請求項２４または２５に記載の情報通信装置。
【請求項２９】
前記通信手段は、着脱可能な記憶装置を用いて、前記第１及び第２の通信装置の間で通信を行うことを特徴とする請求項２４または２５に記載の情報通信装置。
【請求項３０】
ネットワークに接続された送信装置と、
前記送信装置から送信された、著作権保護のための暗号化を行った電子データを、前記ネットワークを介して受信する受信装置と、を備える通信システムにおいて、
前記送信装置及び前記受信装置の少なくとも一方は、
識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、
受信された前記固有の識別情報を登録する識別情報登録手段と、
前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、
前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる認証鍵交換処理手段と、を備えることを特徴とする通信システム。
【請求項３１】
ネットワークに接続された送信装置と、前記送信装置から送信された、著作権保護のための暗号化を行った電子データを前記ネットワークを介して受信する受信装置と、の間で、電子データを伝送する制御を行うデータ伝送制御プログラムにおいて、
識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信するステップと、
受信された前記固有の識別情報を登録するステップと、

前記他の通信装置が前記固有の識別情報を登録しているか否かを判断するステップと、
前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させるステップと、を実行させるためのデータ伝送制御プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、送信装置と受信装置との間で、著作権保護を図る必要のある電子データを送受信する情報通信装置、通信システム及びデータ伝送制御プログラムに関する。

【従来の技術】

【０００２】

デジタル情報家電と呼ばれる商品が増加している。これら商品は、デジタル放送の開始などに伴って普及が期待されており、デジタル放送対応テレビやセットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダなどのデジタルデータやデジタルコンテンツを扱う種々の商品が含まれている。

【０００３】

これら商品の普及に伴って考慮すべき問題の一つはコンテンツの著作権保護である。デジタルデータは、コピー時の品質劣化がないなどの利点がある一方で、不正コピーが容易であるなどの欠点がある。

【０００４】

このため、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機能やデータの暗号化の機能が設けられている。

【０００５】

ここで、ある送信装置から著作権保護が必要なAVデータを受信装置に伝送する場合を想定する。この場合、注意すべきことは、個人（あるいは、拡大解釈して家族）の楽しむ範囲内でAVデータをやり取りするのが著作権保護の前提であり、他人間間でのAVデータのやり取りは、視聴料や著作権料等の支払等が伴わない限り、行うべきではないという点である。

【０００６】

ネットワーク上で著作権保護を図る仕組みとして、DTCP（Digital Transmission Content Protection）が知られている。DTCPは、IEEE1394やUSBなどでデファクトスタンダードになっている著作権保護方式である。DTCPでは、著作権保護が必要なAVデータなどのコンテンツに対して、送信装置と受信装置との間で認証・鍵交換処理を行い、AVデータを暗号化して伝送する（非特許文献１参照）。

【０００７】

一般に、伝送系における著作権保護では、以下の処理手順でAVデータを伝送する。

【０００８】

まず、送信装置と受信装置との間で、AVデータを送受信するためのコマンドを発行する。例えば、AV制御コマンドの一つである再生コマンドを、受信装置が送信装置に対して発行する。

【０００９】

次に、AVデータに対して著作権保護のための暗号化を施した上で、送信装置から受信装置に対してAVデータの転送を始め、それに前後して、送信装置と受信装置との間で、著作権保護のための認証・鍵交換処理を行う。

【００１０】

認証・鍵交換処理に成功すると、送信装置と受信装置との間でAVデータの暗号鍵を共有できるようになるか、あるいは送信装置と受信装置が暗号鍵を計算できるようになり、受信装置は受信した暗号化AVデータの復号及び再生を行う。

【００１１】

AVデータの転送を、IP(インターネットプロトコル)上にて行うようにすれば、ウェブ等

の様々なアプリケーションと連携でき、ウェブブラウザ等の資産も活用でき、種々のネットワーク形態に対応させることもできる。

【００１２】

このため、MPEG等で圧縮されたAVデータを伝送するプロトコルとして、IP（より具体的には、IPv4またはIPv6）を用いることが多い。より具体的なプロトコルとしては、例えばRTP(Real Time Transport Protocol) やHTTP(Hyper Text Transport Protocol)が用いられる。

【非特許文献１】http://www.dtcp.com

【発明の開示】

【発明が解決しようとする課題】

【００１３】

しかしながら、IPでは、具体的なネットワークの形態に関係なく、IPパケットを伝送できるため、セキュリティ上問題が生じる。すなわち、IPには、VPN（Virtual Private Network：仮想プライベートネットワーク）といった、遠隔のIPネットワーク同士を論理的に接続する技術がある。この技術を用いると、例えばA地区のXさん宅のホームネットワークと、(A地区とは物理的に離れた)B地区のYさん宅のホームネットワークを論理的に接続し、この上でIPパケットの転送が可能となる。つまり、Xさん宅のホームネットワークとYさん宅のホームネットワークとが、あたかも1つのホームネットワークであるかのような形でのネットワークの運用が可能である。

【００１４】

著作権法等では、「個人の楽しむ範囲内」でのAVデータのコピー等は許容されているが、「他人同士」のコピー等は許容していない。しかし、上記のような技術（例えばVPN技術）を用いることにより、「他人同士のネットワークでも、論理的に1つのネットワークであると見せかけること(構成すること)」が可能になり、著作権法等に違反する機器を提供してしまうおそれがある。

【００１５】

本発明は、このような点に鑑みてなされたものであり、その目的は、著作権保護を図りつつ、著作権保護の必要な電子データを有効利用できるようにした情報通信装置、通信システム及びデータ伝送制御プログラムを提供することにある。

【課題を解決するための手段】

【００１６】

上述した課題を解決するために、本発明は、他の通信装置との間で、著作権保護のための暗号化された電子データを伝送する情報通信装置において、ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、前記他の通信装置が予め定めた距離的な条件を満たす場合、または前記他の通信装置と共通の識別情報を携帯装置から受信した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【００１７】

また、本発明は、他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【００１８】

また、本発明は、他の通信装置から送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、ネットワークを介して取得した前記他の通信装

置の装置識別情報を登録する識別情報管理手段と、前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【００１９】

また、本発明は、送信装置と、前記送信装置から送信された、著作権保護のための暗号化を行った電子データを受信する受信装置と、を備える通信システムにおいて、前記送信装置及び前記受信装置の少なくとも一方は、ネットワークを介して取得した他方の装置の装置識別情報を登録する識別情報管理手段と、前記他方の装置が所定の有限範囲内のネットワークに接続されていると認識できる場合に、該他方の装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他方の装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【００２０】

また、本発明は、ネットワークを介して他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、受信された前記固有の識別情報を登録する識別情報登録手段と、前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第１の認証鍵交換処理手段と、を備える。

【００２１】

また、本発明は、他の通信装置からネットワークを介して送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、受信された前記固有の識別情報を登録する識別情報登録手段と、前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第１の認証鍵交換処理手段と、を備える。

【００２２】

また、本発明は、ネットワークを介して著作権保護のための暗号化された電子データを伝送する第１及び第２の通信装置に対して、識別情報を送信する情報通信装置であって、前記第１及び第２の通信装置が前記電子データを伝送するのに必要な固有の識別情報を保持する識別情報保持手段と、前記第１及び第２の通信装置に対して前記固有の識別情報を送信する通信手段と、を備える。

【００２３】

また、本発明は、ネットワークに接続された送信装置と、前記送信装置から送信された、著作権保護のための暗号化を行った電子データを、前記ネットワークを介して受信する受信装置と、を備える通信システムにおいて、前記送信装置及び前記受信装置の少なくとも一方は、識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、受信された前記固有の識別情報を登録する識別情報登録手段と、前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる認証鍵交換処理手段と、を備える。

【発明の効果】

【００２４】

以上詳細に説明したように、本発明によれば、他の通信装置が有限範囲内のネットワークに接続されている場合のみ、該他の通信装置の装置識別情報を登録するため、電子データの伝送先を限定することができ、電子データの著作権保護を確実に図ることができる。

【発明の実施の形態】

【００２５】

以下、本発明に係る情報通信装置、通信システム及びデータ伝送制御プログラムについて、図面を参照しながら具体的に説明する。

【００２６】

（第１の実施形態）

図１は本発明に係る通信システムの第１の実施形態の概略構成を示すブロック図である。図１の通信システムは、個人宅内で主にAVデータを送受信することを目的としており、ホームネットワーク１に接続された送信装置２及び受信装置３を備えている。

【００２７】

ホームネットワーク１として、例えばIEEE802.11に準拠した無線LAN、イーサネット（登録商標）またはIEEE1394ネットワークなどの種々のネットワーク形態が採用可能である。ホームネットワーク１には送信装置２や受信装置３以外の装置が接続されていてもよいが、簡略化のため、ここでは省略している。ホームネットワーク１上でインターネットプロトコル（IP）が使用されている場合、IPv4でもよいし、IPv6でもよい。

【００２８】

送信装置２と受信装置３との間で送受信されるAVデータは、著作権保護が必要なAVデータであり、適切な著作権保護を施した状態で転送される。本実施形態では、ネットワーク上の著作権保護を実現する方式として、DTCPを仮定するが、DTCP以外の著作権保護の仕組みを採用してもよい。なお、DTCPについては、http://www.dtcp.comを参照されたい。

【００２９】

本実施形態では、送信装置２と受信装置３との間で、あらかじめ「登録」の手順を設け、互いの装置、あるいは、一方の装置が他方の装置を「登録」する。この「登録」が終了していない装置間では、AVデータの伝送、暗号化されたAVデータの復号化、及び認証・鍵交換処理の完了を許可しない、という仕組みを導入する。

【００３０】

具体的には、異なるホームネットワーク１間では、パケットの伝送に時間がかかることが多く、また異なるホームネットワーク１同士を接続する場合、通常はルータ網（公衆インターネット）が間に入る等の特性を利用して、登録用のパケットの交換が一定時間以内に終了しない場合には、登録を完了させる。また、登録に用いるパケットとして、IPパケットでなく、物理ネットワークレイヤ等のパケット（例えば、イーサネット（登録商標）パケットや無線レイヤパケット）を用いる。

【００３１】

図２は送信装置２の一実施形態の概略構成を示すブロック図である。図２の送信装置２は、ネットワークインターフェース部１１と、通信処理を実行する通信処理部１２と、送信装置２自身のDTCPデバイスIDを記録するDTCPデバイスID記録部１３と、ネットワークを介して取得した同じ宅内の他の通信装置のデバイスIDを登録するID管理部１４と、ID管理部１４にデバイスIDを登録する制御を行う事前登録処理部１５と、他の通信装置からデバイスIDが通知されるまでの時間を計測する時計１６と、著作権保護を図るためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部１７と、送信するデータを暗号化する暗号処理部１８と、受信装置３に送信するAVデータやDTCP管理データを通信パケットに変換するパケット処理部１９と、AVデータを蓄積するコンテンツ供給部２０とを備えている。

【００３２】

事前登録処理部１５は、宅内の他の通信装置にデバイスIDの送信要求を行ってからデバイスIDの応答があるまでの時間を時計１６で計測し、その時間が所定時間以内であれば、ID管理部１４にデバイスIDを登録する。ID管理部１４は、登録されたデバイスIDのリスト（以下、IDリスト）を有し、事前登録処理部１５からデバイスIDの登録要求があると、そ

のIDがIDリストに登録されていなければ、IDリストに加える。

【００３３】

図３はIDリストの一例を示す図である。IDリストは、必須項目として他の通信装置のDTCPデバイスIDを登録し、オプション項目として例えば、RTT（Round Trip Time）、固有ID（例えば、MACアドレス）及び最終利用日時（他の通信装置と最後に通信を行った日時）を登録する。

【００３４】

IDリストには、N（Nは所定の整数）個までのデバイスIDを登録することができる。新たなデバイスIDの登録要求があったときに、すでにＮ個のデバイスIDが登録されている場合には、新たなデバイスＩＤの登録を拒否するか、あるいは最も長い期間通信を行っていない他の通信装置のデバイスIDか、あるいは最も古くに登録されたデバイスIDを削除して、新規のデバイスIDを登録できるようになっていてもよい。また、ユーザが何らかのユーザインタフェースを介して、任意のデバイスIDを削除できるようにしてもよい。

【００３５】

ここで、DTCPデバイスIDとは、DTCPデバイスの識別番号である。全世界のDTCPデバイスは、それぞれ固有のIDをもつのが望ましい。DTCPデバイスIDは、機器証明書（Certificate）と呼ばれる、「その機器が、正しくライセンスされた機器であることの証明書」の中に含まれるIDでもよい。機器証明書には、デジタル署名等が含まれ、これを検証することにより、正しい機器証明書であるか否かを確認することができる。

【００３６】

図４は本発明に係る受信装置３の内部構成を示すブロック図である。図４の受信装置３は、ネットワークインターフェース部２１と、通信処理を実行する通信処理部２２と、受信装置３自身のDTCPデバイスIDを記録するDTCPデバイスID記録部２３と、ネットワークを介して取得した同じ宅内の他の通信装置のデバイスIDを登録するID管理部２４と、ID管理部２４にデバイスIDを登録する制御を行う事前登録処理部２５と、他の通信装置からデバイスIDが通知されるまでの時間を計測する時計２６と、著作権保護を図るためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部２７と、受信したデータを復号化する暗号処理部２８と、受信された信号をAVデータに変換するパケット処理部２９と、AVデータを蓄積するコンテンツ供給部３０とを備えている。

【００３７】

図５及び図６は送信装置２と受信装置３との間で行われる第１の実施形態におけるAVデータの伝送処理手順を示すシーケンス図である。図５及び図６のシーケンス図は、送信装置２と受信装置３の各ユーザが「登録ボタン」を押すか、「登録アイコン」をクリックすることにより開始される（ステップＳ１１，Ｓ１２）。

【００３８】

なお、送信装置２と受信装置３のいずれか一方のみが開始のアクションを行うことで、図５の処理を開始してもよい。あるいは、送信装置２と受信装置３の電源をオンしたときに、自動的に登録モードに設定されて、図５の処理が開始されてもよい。

【００３９】

いずれにしても、「登録ボタンを押した装置同士」、あるいは「登録ボタンを押した通信装置とその他の通信装置（通常は電源がオンしている通信装置）」との間で登録処理が行われることになる。

【００４０】

図５では、送信装置２と受信装置３の二装置間での登録について説明したが、同時に３つ以上の通信装置の登録を行ってもよい。

【００４１】

登録処理が開始されると、送信装置２は時計による時間計測を開始（タイマオン）し（ステップＳ１３）、IDリストに登録する目的で、受信装置３に対してデバイスID送信要求パケットを送信する（ステップＳ１４）。このパケットは、イーサネット（登録商標）フレームか無線レイヤフレーム（データリンクレイヤフレームまたは物理レイヤフレーム）

で送信される。デバイスID送信要求パケットには、送信装置２が選択した乱数やタイムスタンプが含まれている。送信装置２は、デバイスID送信要求パケットをネットワーク上でブロードキャストしてもよい。この場合、イーサネット（登録商標）ブロードキャストアドレスを宛先イーサネット（登録商標）アドレスとして用いる。

【００４２】

デバイスID送信要求パケットを受けて、受信装置３は、送信装置２に対してデバイスID応答パケットを送信する（ステップＳ１５）。このデバイスID応答パケットも、イーサネット（登録商標）フレームか無線レイヤフレームで送信される。受信装置３は、送信装置２からのデバイスID送信要求パケットに含まれていた乱数やタイムスタンプをそのままデバイスID応答パケットに含めてもよい。これにより、送信装置２は、どの要求パケットに対する応答かを知ることができ、時計１６による時間計測を行いやすくなる。

【００４３】

なお、受信装置３からデバイスID送信要求パケットを送信し、そのパケットを受信した送信装置２がデバイスID応答パケットを受信装置３に送信してもよい。この場合、パケットの応答までの時間計測は受信装置３で行うことになる。

【００４４】

送信装置２内の事前登録処理部１５は、デバイスID応答パケットが所定時間Ｔ以内に受信された場合、受信装置３のデバイスIDをID管理部２４に登録し、所定時間Ｔ以内に受信されなかった場合、登録失敗と判断して、ID管理部２４への登録を行わない（ステップＳ１６）。

【００４５】

デバイスIDの登録に失敗した場合、ユーザに対して、「デバイスIDの登録は、もっと近距離で同一リンクレイヤネットワーク上で行う必要がある」ことを通知する必要がある。このため、ユーザに対して、送信装置２及び受信装置３を同じイーサネット（登録商標）スイッチに差込んで登録を行うよう誘導したり、直接イーサネット（登録商標）ケーブルで接続して登録を行うよう誘導したり、ネットワーク上のトラフィックを一時的に少なくするよう（例えば、他の通信装置のAVデータの伝送を止めるよう）誘導したり、送信装置２または受信装置３が起動中の他のアプリケーションを停止して処理負担を軽減するよう誘導したりする。

【００４６】

ステップＳ１６の処理が終了した後、今度は受信装置３が時計２６による時間計測を開始し（ステップＳ１７）、送信装置２に対してデバイスID送信要求パケットを送信する（ステップＳ１８）。この要求を受けて、送信装置２はデバイスID応答パケットを送信する（ステップＳ１９）。

【００４７】

受信装置３は、送信装置２からのデバイスID応答パケットが所定時間Ｔ以内に受信された場合には送信装置２のデバイスIDをID管理部に登録し、所定時間Ｔ以内に受信されなかった場合は、送信装置２のデバイスIDの登録を行わない（ステップＳ２０）。

【００４８】

以上の手順で、送信装置２及び受信装置３は登録モードを終了し（ステップＳ２１，Ｓ２２）、認証・鍵交換処理を行う（図６のステップＳ２３～Ｓ２９）。

【００４９】

まず、受信装置３は、送信装置２に対して、IPパケットを利用して認証・鍵交換要求を行う（ステップＳ２３）。このとき、自己のデバイスIDもIPパケットに含めて送信する。

【００５０】

受信装置３からのIPパケットを受信した送信装置２は、受信装置３のデバイスIDがID管理部１４に登録されているか否かを確認し（ステップＳ２４）、確認が取れると、受信装置３に対して、IPパケットを利用して認証・鍵交換要求を行う（ステップＳ２５）。このとき、自己のデバイスIDもIPパケットに含めて送信する。

【００５１】

送信装置２からのIPパケットを受信した受信装置３は、送信装置２のデバイスIDがID管理部２４に登録されているか否かを確認し（ステップＳ２６）、確認が取れると、送信装置２と受信装置３との間で、認証・鍵交換手続を行う（ステップＳ２７）。

【００５２】

認証・鍵交換手続が成功すると、送信装置２と受信装置３はコンテンツ暗号鍵を共有し（ステップＳ２８，Ｓ２９）、送信装置２はコンテンツの暗号化を行う（ステップＳ３０）。

【００５３】

次に、送信装置２は受信装置３に対して、暗号化されたAVデータをRTPまたはHTTPにて伝送する（ステップＳ３１）。このAVデータを受信した受信装置３は、コンテンツの復号化を行う（ステップＳ３２）。

【００５４】

なお、送信装置２と受信装置３のいずれか一方で、すでにデバイスIDの登録手続が終わっている場合には、図５のステップＳ１３～Ｓ１６またはＳ１７～Ｓ２０を省略してもよい。

【００５５】

デバイスIDの登録要求と登録応答を行う際に、なりすまし（man in the middle attack）を防止する手順を設けてもよい。この場合、例えば図５のステップＳ１４～Ｓ１６の代わりに図７のような処理を行う。

【００５６】

まず、送信装置２は受信装置３に対して、イーサネット（登録商標）フレームまたは無線レイヤフレームにて乱数送信パケットを送信する（ステップＳ４１）。乱数送信パケットには、送信装置２が生成した乱数ｒが含まれている。

【００５７】

この乱数送信パケットを受信した受信装置３は、乱数ｒと自己のデバイスIDを用いて署名を計算する（ステップＳ４２）。次に、受信装置３は送信装置２に対して、イーサネット（登録商標）フレームまたは無線レイヤフレームにて乱数受信通知を行う（ステップＳ４３）。

【００５８】

この通知を受けた送信装置２は、時計による時間計測を開始し（ステップＳ４４）、受信装置３に対して、イーサネット（登録商標）フレームまたは無線レイヤフレームにてデバイスID要求パケットを送信する（ステップＳ４５）。このパケットには、上述した乱数ｒが含まれている。

【００５９】

このパケットを受信した受信装置３は、送信装置２に対して、乱数ｒ、自己のデバイスID及び署名を含むデバイスID応答パケットを送信する（ステップＳ４６）。

【００６０】

送信装置２は、デバイスID要求パケットを送信してからデバイスID応答パケットが受信されるまでの時間が所定時間Ｔ以内か否かを判断し、所定時間Ｔ以内であれば、受信装置３のデバイスID＝ｂをID管理部に登録し、所定時間Ｔ以内に受信されなかった場合は、ID管理部への登録を行わないようにする（ステップＳ４７）。

【００６１】

このように、第１の実施形態では、デバイスIDの登録要求を行ってから所定時間以内に応答が返ってきた場合のみ、他の通信装置（受信装置３または送信装置２）の登録を行うようにしたため、有限の範囲内の通信装置との間でのみAVデータの伝送を行うことができ、簡易な処理でAVデータの著作権保護を図ることができる。

【００６２】

（第２の実施形態）

第２の実施形態は、受信装置３が送信装置２に対して認証・鍵交換要求を行った後に、送信装置２が受信装置３にデバイスID要求パケットを送信するものである。

【００６３】
第２の実施形態の送信装置２及び受信装置３は、それぞれ図３及び図４と同様に構成されるため、構成の説明を省略する。
【００６４】
図８は第２の実施形態におけるAVデータの伝送処理手順を示すシーケンス図である。まず、受信装置３から送信装置２に対して認証・鍵交換要求を行う（ステップＳ５１）。送信装置２は、認証・鍵交換要求を行った受信装置３がID管理部に登録されていないことを確認すると（ステップＳ５２）、時計による時間計測を開始し（ステップＳ５３）、受信装置３に対してイーサネット（登録商標）フレームまたは無線レイヤフレームにてデバイスID要求パケットを送信する（ステップＳ５４）。
【００６５】
このパケットに応答して、受信装置３は、送信装置２に対してイーサネット（登録商標）フレームまたは無線レイヤフレームにてデバイスID応答パケットを送信する（ステップＳ５５）。
【００６６】
次に、送信装置２は、デバイスID要求パケットを送信してからデバイスID応答パケットが所定時間Ｔ以内に返ってきた場合、受信装置３のデバイスID（＝ｂ）をID管理部１４に登録し、所定時間Ｔ以内に返って来なかった場合、登録を行わない（ステップＳ５６）。
【００６７】
次に、今度は、受信装置３は同様の手順で送信装置２のデバイスIDの登録手続を行う（ステップＳ５７～Ｓ６０）。以下、図６のステップＳ２１～Ｓ３２と同様の処理を行う。
【００６８】
なお、送信装置２と受信装置３のいずれか一方で、すでにデバイスIDの登録手続が終わっている場合には、図８のステップＳ５２～Ｓ５６またはＳ５７～Ｓ６０を省略してもよい。
【００６９】
このように、第２の実施形態では、認証・鍵交換要求のあった後にデバイスIDの登録要求を行うため、不必要にデバイスIDの登録要求とその応答を行わなくて済み、通信トラフィックを低減できる。
【００７０】
（第３の実施形態）
第３の実施形態は、第１及び第２の実施形態と異なり、短距離無線装置から送信されたIDを登録している送信装置と受信装置との間でのみAVデータを伝送できるようにしたものである。
【００７１】
図９は本発明に係る通信装置の第３の実施形態の概略構成を示すブロック図である。図９の通信システムは、図１の構成に加えて、赤外線リモートコントローラ（以下、リモコン）や無線タグなどからなる短距離無線装置４を備えている。
【００７２】
本実施形態の送信装置２ａ及び受信装置３ａは、それぞれ短距離無線装置４と無線通信を行って、短距離無線装置４から送信されたグローバルユニークなID（以下、短距離IDと呼ぶ）を登録する。この短距離IDが登録されている送信装置２ａと受信装置３ａの間でのみ、AVデータの伝送が行えるようにする。より具体的には、上述のIDが登録されていない送信装置２ａと受信装置３ａの間では、認証鍵交換（あるいはコンテンツの送受信）が成功しないようにする。
【００７３】
個々の短距離無線装置４は、短距離IDを保持しており、このIDを、短距離無線通信を利用してのみ、送信装置２ａと受信装置３ａにそれぞれ送信する。ここで、短距離とは、例えば赤外線を利用する場合には、赤外線が届く範囲（例えば数ｍ）であり、また無線タグを利用する場合には、電波が届く範囲（例えば数ｃｍ）である。

【００７４】
図１０は図９の送信装置２ａの概略構成の一例を示すブロック図である。図１０では、図２と共通する構成部分には同一符号を付しており、以下では、図２との相違点を中心に説明する。
【００７５】
図１０の送信装置２ａは、図２と同様に、ネットワークインターフェース部１１、通信処理部１２、DTCPデバイスID記録部１３、ID管理部１４、DTCP認証鍵交換処理部１７、暗号処理部１８、パケット処理部１９及びコンテンツ供給部２０を備えている。この他、図１０の送信装置２ａは、短距離無線通信のための短距離無線インターフェース部４１と、短距離無線装置４との間で認証鍵交換を行う短距離認証鍵交換処理部４２と、短距離無線通信により取得した短距離IDを登録する短距離ID管理部４３と、短距離ID管理部４３に短距離IDを登録する制御とを行う事前登録処理部４４と、短距離IDの登録が終了したことをユーザに通知する登録終了通知処理部４５と、短距離ＩＤの登録時にのみ短距離無線インタフェース部４１やその周辺部に電源電圧を供給する電源制御部４６とを備えている。
【００７６】
短距離ID管理部４３と事前登録処理部４４はそれぞれ、セキュリティ保持のために、短距離IDを暗号化する暗号通信処理部４３ａ，４４ａを持っていてもよい。これにより、短距離ID管理部４３と事前登録処理部４４との間のデータバス上で短距離IDを不正に取得されるおそれがなくなる。すなわち、短距離無線インターフェース部４１、短距離無線認証鍵交換処理部４２及び事前登録処理部４４などが、例えば、赤外線モジュールや無線タグモジュールなどの形態でモジュール化されていて、各モジュールがPCIバス等の汎用バスに接続されて場合で、かつ短距離ID管理部４３やDTCP認証鍵交換処理部１７がMPU側のソフトウェア等で処理される場合、事前登録処理部４４と短距離ID管理部４３との間でのデータ伝送は汎用バスを介して行うことになる。したがって、短距離ID等が暗号化されていないと、このID等を汎用バス上で不正に取得されて、ID等の不正利用や不正コピーなどが行われるおそれがある。
【００７７】
このことから、短距離ID管理部４３と事前登録処理部４４にそれぞれ暗号通信処理部４３ａ，４４ａを設けて、短距離ID等を暗号化して伝送するのが望ましい。なお、暗号通信処理部４３ａ，４４ａは、ハードウェアで構成してもよいし、ソフトウェアで暗号化するAPIを用意して、ソフトウェアでID等を暗号化してもよい。
【００７８】
また、この暗号通信処理部４３ａと４４ａ間でのやり取りが、一定時間以内に行われているかどうかを計測する機能が、これら暗号通信処理部４３ａと４４ａに内蔵されていても良い。これは、短距離ＩＤ管理部４３と事前登録処理部４４との物理的な距離が、一定長さ以内（例えば、同じ筐体の中、あるいは、短距離無線の処理部がＵＳＢドングル等の外付け部品として構成されており、この外付け部品と短距離ＩＤ管理部４３との物理的な距離が一定長さ以内）であることを確認するための機能である。
【００７９】
この場合の外付け部品とは、例えば、短距離無線インターフェース部４１と、短距離認証鍵交換処理部４２と、事前登録処理部４４とで構成される。この機能がない場合、外付け部品を遠隔地に配置し、短距離ＩＤ管理部４３と外付け部品との間をインターネット等の公衆網（広域網）で接続して、遠隔地から登録を行う、という攻撃が考えられるので、これを未然に防止する効果がある。
【００８０】
また、短距離無線に関する機能（例えば、短距離無線インターフェース部４１と、短距離認証鍵交換処理部４２と、事前登録処理部４４）は、短距離ＩＤの登録の時以外には使うことのない機能である可能性がある。このため、これらの機能は、短距離ＩＤの登録時以外には通電しない等の工夫をすることにより、省電力を図ることが可能になる。これを制御するのが電源制御部４６である。電源制御部４６は、ユーザが短距離IDの登録ボタン

等を押したことを検知して、電源制御を行う。

【００８１】

ここで、短距離無線IDとは、短距離無線装置４の識別番号であり、DTCPと同じライセンス機関が、世界唯一の値となるように割り当てる識別番号であってもよい。また、短距離無線IDは、DTCPのデバイスIDと同様に、機器証明書（Certificate）と呼ばれる「その機器が、正しくライセンスされた機器であることの証明書」の中に含まれるIDであってもよい。この機器証明書には、デジタル署名等が含まれ、これを検証することにより、正しい機器証明書であるかどうかを確認することができる。

【００８２】

図１１は受信装置３ａの一実施形態の概略構成を示すブロック図である。図１１では、図４と共通する構成部分には同一符号を付しており、以下では、図４との相違点を中心に説明する。

【００８３】

図１１の受信装置３ａは、図４と同様に、ネットワークインターフェース部２１、通信処理部２２、DTCPデバイスID記録部２３、DTCP認証鍵交換処理部２７、暗号処理部２８、パケット処理部２９及びコンテンツ供給部３０を備えている。この他、図１１の受信装置３ａは、短距離無線通信のための短距離無線インターフェース部５１と、短距離無線装置４との間で認証鍵交換を行う短距離認証鍵交換処理部５２と、短距離無線通信により取得した短距離IDを登録する短距離ID管理部５３と、短距離ID管理部５３に短距離IDを登録する制御を行う事前登録処理部５４と、短距離IDの登録が終了したことをユーザに通知する登録終了通知処理部５５と、短距離ＩＤの登録時にのみ短距離無線インタフェース部、あるいはその周辺を稼動する（電源をＯＮにする）電源制御部５６とを備えている。

【００８４】

図１２は送信装置２ａや受信装置３ａ内の短距離ID管理部４３，５３のデータ構造を示す図である。短距離ID管理部４３，５３は、短距離IDの値が必須項目として登録され、それ以外に、オプション項目として、各IDごとに、RTT（Round Trip Time）、DTCPデバイスID及び登録日時などが登録される。

【００８５】

図１３は短距離無線装置４を赤外線リモコン装置で実現した場合の内部構成の一例を示すブロック図であり、赤外線リモコン装置の例を示している。図１３の赤外線リモコン装置は、赤外線通信インターフェース部６１と、AV機器を初期化するためのAV機器初期化処理部６２と、AV機器を制御するためのAV機器制御処理部６３と、自装置の短距離IDを記録する短距離ID記録部６４と、短距離ID記録部６４にIDを登録する制御を行う事前登録処理部６５と、短距離ID記録部６４に短距離IDを記録した回数を計測する登録回数カウンタ６６と、送信装置２ａ及び受信装置３ａとの間で認証鍵交換を行う短距離無線認証鍵交換処理部６７と、ユーザインタフェース部６８とを備えている。

【００８６】

ここで、赤外線通信インタフェース部６１は、短距離ＩＤ登録用双方向赤外線インタフェース６１ａと、ＡＶ機器制御用片方向赤外線インタフェース６１ｂとを内蔵していてもよい。これは、ＡＶ機器を制御するための赤外線リモコンのインタフェースは一般に片方向であるのに対して、後述するように本実施形態の短距離ＩＤを登録するための赤外線インタフェースは双方向である。これら２つの機能を実現するためには、赤外線通信インタフェース部６１は、２つの赤外線インタフェース６１ａと６１ｂを備える必要がある。これらの２つの赤外線インタフェースは、２つ以上の個別部品で構成されていても良いし、１つの個別部品に封止されていても良い。短距離ＩＤ登録用双方向赤外線インタフェース６１ａは短距離無線認証・鍵交換処理部６７とＡＶ機器初期化処理部６２と接続している。一方、ＡＶ機器制御用片方向赤外線インタフェース６１ｂは、ＡＶ機器制御処理部６３と接続されている。これら２つの赤外線インタフェース６１ａ，６１ｂは、異なる赤外線の周波数や、コマンド体系、パケットフォーマット等を使用してもよい。

【００８７】

一方、図１４は短距離無線装置４を無線タグ装置で実現した場合の内部構成の一例を示すブロック図である。図１４の無線タグ装置は、無線タグ通信インターフェース部７０と、AV機器初期化処理部７１と、短距離無線認証鍵交換処理部７２と、事前登録処理部７３と、登録回数カウンタ７４と、短距離ID記録部７５と、ユーザインタフェース部７６とを備えている。

【００８８】

無線タグ装置は、受信電波により生成された電力を利用して無線信号を送信するため、バッテリが不要となり、経済的である。図１４では省略しているが、無線タグ装置内には、受信電波により生成された電力を蓄積するキャパシタが設けられている。

【００８９】

図１５は送信装置２ａ及び受信装置３ａにおける短距離IDの登録処理手順を示すシーケンス図である。以下、図１５に基づいて短距離IDの登録処理手順を説明する。短距離無線装置４から送信装置２ａ（または受信装置３ａ）に短距離IDを送信する際、ユーザが短距離無線装置４の図１３に示すボタン６８ａを押下すると、短距離無線装置４は登録モードに入る（ステップＳ７１）。また、ユーザは、短距離IDを送信すべき対象である送信装置２ａ（または受信装置３ａ）のボタンも押下し、短距離無線装置４を送信装置２ａ（または受信装置３ａ）に向ける。以上の手順により、送信装置２ａ（または受信装置３ａ）は登録モードに入る（ステップＳ７２）。

【００９０】

この登録モードに入った場合に、電源制御部５６（または６６）は、送信装置２ａ（または受信装置３ａ）における短距離無線インタフェース部４１（または５１）およびその周辺部を通電するようにしてもよい。

【００９１】

このように、本実施形態では、短距離IDの登録を行う際、ユーザ自身が送信装置２ａや受信装置３ａのボタンを押下する必要があるため、送信装置２ａから離れた場所にいる受信装置３ａに、インターネット等を介してAVデータを送信するおそれがなくなる。

【００９２】

次に、ユーザは、短距離無線装置４を送信装置２ａ（または受信装置３ａ）に向けるか近づけて、短距離ID登録ボタンを押下する（ステップＳ７３）。これにより、短距離無線装置４と送信装置２ａ（または受信装置３ａ）との間で認証鍵交換が行われ、正規のライセンス機関が認めた装置であることを互いに認証する（ステップＳ７４）。その際、必要に応じて、公開鍵などの鍵交換も行う。この手順は、後に詳述する。

【００９３】

次に、短距離無線装置４は、短距離IDを送信装置２ａ（または受信装置３ａ）に送信して登録を行った回数を計測する登録回数カウンタがゼロより大きいか否かを判断する（ステップＳ７５）。登録回数カウンタがゼロより大きければ、所定回数以下の登録しか行っていないことを示しており、この場合は送信装置２ａ（または受信装置３ａ）に短距離IDを送信する（ステップＳ７６）。登録回数カウンタがゼロの場合には、所定回数の登録をすでに行ったことを示しており、この場合は短距離IDの送信を中止する。

【００９４】

短距離無線装置４は、送信装置２ａ（または受信装置３ａ）に短距離IDを送信した場合には、登録回数カウンタを「１」だけデクリメントする（ステップＳ７７）。

【００９５】

短距離IDを受信した送信装置２ａ（または受信装置３ａ）は、その短距離IDを短距離ID管理部４３，５３に伝送する（ステップＳ７８）。伝送途中で短距離IDを不正取得されないように、上述したように、例えば短距離IDを暗号化したり、署名を付けて改ざんされたか否かを確認できるようにしてもよい。また、この短距離ＩＤ管理部４３，５３への伝送が一定時間以内に行われたかどうかの測定を行っても良い。

【００９６】

次に、短距離ID管理部４３，５３に登録されている短距離IDの数が所定数Ｎ未満か否か

を確認し（ステップＳ７９）、所定数以下であれば、受信された短距離IDの登録を行う。一方、すでに所定数Ｎの短距離IDが登録されている場合には、上述したように、最も長い間登録された短距離IDを削除するなどして、新たな短距離IDを登録してもよい。

【００９７】

以上の手順により、短距離無線装置４と送信装置２ａ（または受信装置３ａ）での登録モードを終了し、終了した旨をビープ音やディスプレイ上への表示等によりユーザに通知する（ステップＳ８０～Ｓ８３）。

【００９８】

送信装置２ａと受信装置３ａは、それぞれが所持する短距離ID管理部４３，５３に短距離IDを登録している。短距離ID管理部４３，５３には、予め定めた所定個数ＮまでのIDを登録することができる。Ｎ個の値は１でもよいが、例えば４、８及び16などの数値が選択されてもよい。仮に、上限であるＮ個まですでに登録されている状態で、新たなIDの登録要求があった場合には、最も過去に登録されたIDを削除する代わりに、新規のIDを登録するなどの手法も考えられるが、所定個数ＮのIDを登録すると、それ以上の登録はできないというのが基本的な考え方である。

【００９９】

短距離ID管理部４３，５３への登録処理は、送信装置２ａと受信装置３ａがそれぞれ個別に行う。すなわち、送信装置２ａと受信装置３ａのそれぞれが、同じ短距離無線装置４を使用して短距離IDの登録を行う。この場合、送信装置２ａと受信装置３ａが互いに近距離にいることを確認できると、さらに望ましい。このような確認ができないと、送信装置２ａは東京にあり、受信装置３ａが大阪にある場合でも、異なる時間に同じ短距離無線装置４を用いて、同じ短距離IDを登録できてしまい、任意の遠隔地同士での遠隔通信が可能になる。

【０１００】

このため、図１３に示すように、短距離無線装置４内に時計６９を設け、送信装置２ａ及び受信装置３ａの登録作業は連続して数分以内に行わないと無効になるようにしてもよい。

【０１０１】

あるいは、短距離無線装置４内にGPS（Global Positioning System）を内蔵し、送信装置２ａと受信装置３ａとの距離が所定長さ以上離れていると予測できる場合は、短距離IDの登録ができないようにしてもよい。

【０１０２】

また、図１０および図１１に示すように、送信装置２ａと受信装置３ａの事前登録処理部４４，５４にRTT（Round Trip Time）を計測するRTT計測部４７，５７をそれぞれ設け、リモコン装置や無線タグ装置とのデータのやり取りに要する時間（RTT）が、一定時間以下で行われている事を確認し、そうでない場合には短距離ＩＤの登録ができないようにしてもよい。RTT計測部４７，５７は、例えば短距離無線装置４に対して特定のパケットを送信し、これに対する応答パケットが返ってくるまでのラウンドトリップ時間を計測する。この計測結果に基づいて、短距離無線装置４までの距離が推定される。

【０１０３】

また、送信装置２ａと受信装置３ａの事前登録処理部４４，５４にそれぞれ時計を設け、リモコン装置や無線タグ装置とのデータのやり取り（RTT）が、一定時間以下で行われていることを確認し、そうでない場合には短距離ＩＤの登録ができないようにしてもよい。

【０１０４】

図１６は認証鍵交換および登録用短距離ID送信処理のシーケンス図である。まず、短距離無線装置４から送信装置２ａ（又は受信装置３ａ）に対して、登録処理の開始を要求するトリガをかける（ステップＳ１１１）。すると、送信装置２ａ（または受信装置３ａ）の事前登録処理部４４，５４は、RTT計測部４７，５７内のタイマをスタートさせ（ステップＳ１１２）、ラウンドトリップ時間（RTT）を測定するためのコマンドを短距離無線

装置４に対して送信する（ステップＳ１１３）。このコマンドには、短距離無線装置４が選択したランダム値Ａｎが共に伝送されても良い。これを受信した短距離無線装置４は、即座にリプライを送信装置２ａ（又は受信装置３ａ）に対して送信する（ステップＳ１１４）。このリプライには、送信装置２ａ（又は受信装置３ａ）が選択したランダム値Ｂｎが共に伝送されても良い。

【０１０５】

これを受信した送信装置２ａ（又は受信装置３ａ）は、RTT計測部４７，５７内のタイマを使って、RTTを計測する（ステップＳ１１５）。この値が、あらかじめ定めた値（例えば数ｍｓ）以下である場合、短距離無線装置４と、送信装置２ａ（又は受信装置３ａ）との間が一定距離以下であると認識し、これに続く認証鍵交換処理を有効とする。もし、このRTTが一定時間以上かかった場合には、短距離無線装置４と送信装置２ａ（又は受信装置３ａ）との間が一定距離以上（間に公衆網が介在し、これらの装置が遠隔地に配置されている可能性がある）と認識し、以降の認証鍵交換処理を無効としても良い。このRTTの計測は、暗号演算やハッシュ演算が発生しないシーケンスにて行っている。このため、暗号演算やハッシュ演算に必要な時間を考慮することなく、厳密な値に近いRTTの値を計測できる、というメリットがある。

【０１０６】

なお、本実施形態においては、送信装置２ａ（又は受信装置３ａ）の側がRTTの計測を行っているが、例えばシーケンスの向きを逆にして、短距離無線装置４の側がRTTの計測を行うようにしても良い。また、送信装置２ａ（又は受信装置３ａ）と、短距離無線装置４の全てがRTTの計測を行うような手順も考えられる。

【０１０７】

次に、短距離無線装置４と送信装置２ａ（又は受信装置３ａ）は、認証鍵交換処理に入る。本実施形態における、この処理は、DTCP標準で既に標準化されている、拡張制限認証(Extended Restricted Authentication)を用いる事とする。即ち、送信装置２ａ（又は受信装置３ａ）からキー選択ベクトルAksvを短距離無線装置４に送信し（ステップＳ１１６）、短距離無線装置４からはその機器証明書（Bcert）とキー選択ベクトル（Bksv）を送信装置２ａ（又は受信装置３ａ）に送信する（ステップＳ１１７）。双方はあらかじめ定められた演算に従って、Ｒ，及びＲ‘の値を計算する（ステップＳ１１８，Ｓ１１９）。

【０１０８】

ここで、SHA-1とは、あらかじめ定められたハッシュ関数である。短距離無線装置４により演算されたＲの値は送信装置２ａ（又は受信装置３ａ）に対して送信される（ステップＳ１２０）。

【０１０９】

送信装置２ａ（又は受信装置３ａ）では、自分で計算したＲ’と、短距離無線装置４から送信されてきたＲの値を比較し（ステップＳ１２１）、この値が一致していたならば、認証鍵交換が成功したものとして、認証鍵Kauthを演算する（ステップＳ１２２，Ｓ１２３）。同じ認証鍵の値Kauthを送信装置２ａ（又は受信装置３ａ）も持つことができるため、この値を鍵として、短距離無線装置４は短距離IDの値（AA）を送信装置２ａ（又は受信装置３ａ）に対して送信する（ステップＳ１２４）。例えば、短距離IDとKauthの値のXORを使ったり、Kauthの値を鍵とした暗号演算の結果を送ったりする等の方法が考えられる。

【０１１０】

DTCPの拡張制限認証には、機器のリボークの仕組みが備わっているため、送信装置２ａ（又は受信装置３ａ）は、特定の短距離無線装置４からの手続きを拒否（リボーク）することが可能である。

【０１１１】

ここで、DTCPの拡張制限認証の手順の詳細は、http://www.dtcp.comのDTCP標準を参照されたい。

【０１１２】
図１７は送信装置２ａと受信装置３ａとの間でAVデータの伝送を行う際の処理手順を示すシーケンス図である。ここでは、送信装置２ａ（デバイスID＝ａとする）と受信装置３ａ（デバイスID＝ｂとする）にそれぞれ、短距離ID管理部４３，５３に共通の短距離ID＝AAが登録されているものとする。
【０１１３】
次に、受信装置３ａは、自己のデバイスID＝ｂと短距離ID＝AAを通知して、送信装置２ａに対して認証鍵交換要求を行う（ステップＳ９１）。
【０１１４】
この要求を受信した送信装置２ａは、短距離ID管理部に短距離ID＝AAが登録されていることを確認し（ステップＳ９２）、自己のデバイスID＝ａと短距離ID＝AAを通知して、受信装置３ａに対して認証鍵交換要求を行う（ステップＳ９３）。
【０１１５】
この要求を受信した受信した受信装置３ａは、短距離ID管理部に短距離ID＝AAが登録されていることを確認し（ステップＳ９４）、送信装置２ａと受信装置３ａとの間で認証鍵交換処理を行う（ステップＳ９５）。
【０１１６】
認証鍵交換に成功すると、送信装置２ａと受信装置３ａはコンテンツ暗号鍵を共有する（ステップＳ９６，Ｓ９７）。この鍵を利用して、送信装置２ａはAVデータを暗号化し（ステップＳ９８）、暗号化されたAVデータを受信装置３ａに送信する（ステップＳ９９）。受信装置３ａは、受信したAVデータをコンテンツ暗号鍵を用いて復号する（ステップＳ１００）。
【０１１７】
なお、ここでコンテンツ暗号鍵の演算に、短距離IDの値を入力として用いる方法も考えられる。
【０１１８】
図１８は、上述したステップＳ９１で受信装置３ａから送信された短距離ID＝AAが送信装置２ａの短距離ID管理部４３に登録されていなかった場合の処理手順を示すシーケンス図である。この場合、送信装置２ａは、短距離ID管理部４３に短距離ID＝AAが登録されていないことを確認して、ビープ音等により、ユーザに短距離IDの登録を促す（ステップＳ１０１）。
【０１１９】
図１９は送信装置２ａと受信装置３ａとの間でAVデータの伝送を行う際の処理手順を示すシーケンス図の別例を示している。この例では、送信装置２ａと受信装置３ａの間でコンテンツ暗号鍵を共有するまでの処理（ステップＳ１３１～Ｓ１３４）は、図１７のDTCP認証鍵交換と同様であり、その後、短距離IDの値の確認を片方、あるいは双方で行う（ステップＳ１３５～Ｓ１３８）。この場合には、従来のDTCP認証鍵交換の手順に変更が加わらないため、短距離IDの値のやり取りを行う追加のコマンドを用意するのみで、従来のコマンドはそのまま利用できるというメリットがある。
【０１２０】
（第４の実施の形態）
第３の実施形態では、短距離無線装置を介してIDの登録を行うが、第4の実施形態では、短距離無線装置を使う代わりに、ICカード（接触型ICカード）やメモリカード等の着脱可能な記憶装置を使ってIDの登録を行う。ここでICカードとは、ICを内蔵した、例えばプラスチックカードであり、クレジットカード大のものや切手大のものなどが考えられる。また、メモリカードとは、例えば、PCMCIAのメモリカード、あるいはSDカードやメモリスティックに代表されるメモリカード等である。形状はカード形状にかかわらず、例えばUSBキーなどの着脱可能な記憶装置であればよい。
【０１２１】
図２０は本発明に係る通信装置の第４の実施形態の概略構成を示すブロック図、図２１

は図２０の送信装置２ｂの内部構成の一例を示すブロック図、図２２は図２０の受信装置３ｂの内部構成の一例を示すブロック図である。第３の実施の形態との差分点は、赤外線リモコンや無線タグなどからなる短距離無線装置の代わりに、ICカード又はメモリカード（以下、総称してICカードと記載）５を用いてIDの登録を行う点である。

【０１２２】

本実施形態の送信装置２ｂ及び受信装置３ｂは、第3の実施形態の送信装置２ａ及び受信装置３ａと比べて、短距離無線インタフェース及び短距離無線認証鍵交換処理部がない代わりに、ICカードインタフェース部３１，３２及びICカード認証鍵交換処理部３３，３４をそれぞれ有する（図２１、図２２）。

【０１２３】

送信装置２ｂと受信装置３ｂは、対応するICカードインタフェース部３１，３２を介してICカード５と通信を行って、ICカード５から送信されたグローバルユニークなID（短距離ID）を登録する。この短距離IDが登録されている送信装置２ｂと受信装置３ｂの間でのみ、AVデータの伝送が行えるようにするのは第３の実施形態と同様である。

【０１２４】

個々のICカードは、短距離IDを保持している。この短距離IDを、送信装置２ｂ、あるいは受信装置３ｂのICカードスロット（ICカードインタフェース部）に挿入（あるいはセット）し、送信する。IDの送信は、ICカードがICカードインタフェース部に物理的に存在する場合にのみなされるため、遠距離からの登録は不可能であると考えられる。

【０１２５】

図２３はICカードの内部構成の一例を示すブロック図である。図２３のICカードは、ICカードインタフェース部８１と、AV機器を初期化するためのAV機器初期化処理部８２と、自装置の短距離IDを記録する短距離ID記録部８３と、短距離ID記録部８３にIDを登録する制御を行う事前登録処理部８４と、短距離ID記録部８３に短距離IDを記録した回数を計測する登録回数カウンタ８５と、送信装置２ｂ及び受信装置３ｂとの間で認証鍵交換を行う短距離無線認証鍵交換処理部８６とを有する。

【０１２６】

図２３のICカードはメモリカードやその他の機能を行うものであってもよく、その場合は、メモリ部や他の処理を行う機能がICカードに搭載される。

【０１２７】

第４の実施形態における短距離IDの登録処理手順や登録のシーケンスや内部の動作等は第３の実施形態と同様であり、第３の実施形態と同様の作用効果が得られる。

【０１２８】

（第５の実施の形態）

第４の実施形態で詳述したIDの登録は、ICカードやメモリカードを介して行っていた。デジタルAV機器の中には、あらかじめICカードのインタフェース部を持ち、「ICカードが刺さっていないと、AV機器として利用できない」機器が存在する。この例が、日本のデジタル放送で広く使われている「B-CASカード」である。このカードには、デジタル放送で送信されてくる（スクランブルがかかった）コンテンツが入力され、このスクランブルを解除して平文のコンテンツにした上で、出力する機能が備わっていたり、内蔵されているID番号（短距離IDとは異なるＩＤ）を使って、受信者の確認に使う等の機能が備わっている。

【０１２９】

デジタル放送機器には、このＩＣカードインタフェース部が必ず備わっており、本発明の短距離ＩＤを書き込むためのＩＣカードと共用できると便利である。本実施形態は、これを実現するものである。

【０１３０】

図２４は本発明に係る通信システムの第５の実施形態の概略構成を示すブロック図、図２５は図２４の受信装置３ｃの内部構成の一例を示すブロック図である。図２４の通信システムは、図２０の通信システムがＩＣカード（又はメモリカード）を使っていたのに対

し、図２５ではB-CASカードを用いている点である。

【０１３１】

図２４の通信システムは、送信装置２ｃと、受信装置３ｃと、送信装置２ｃや受信装置３ｃに挿入可能なB-CASカード６とを備えている。

【０１３２】

本実施形態では、受信装置３ｃがデジタル放送受信機能付の機器（例えばディスプレイ）である場合について説明する。

【０１３３】

図２５に示すように、受信装置３ｃは、B-CASカードインタフェース部３５と、B-CASカード認証・鍵交換処理部３６とを有する。送信装置２ｃも、B-CASカードインタフェース部やB-CASカード認証・鍵交換処理部を持っていてもよい。

【０１３４】

B-CASカードインタフェース部３５は、短距離ＩＤの登録のための機能を持つ他に、先に述べたB-CASカード特有の機能（スクランブル処理や受信者確認等）を有する。

【０１３５】

図２６はB-CASカード６の内部構成の一例を示すブロック図である。図２６のB-CASカードは、B-CASカードインタフェース部９１と、B-CAS処理部９２と、AV機器初期化処理部９３と、短距離無線認証・鍵交換処理部９４と、事前登録処理部９５と、登録回数カウンタ９６と、短距離ID記録部９７とを有する。

【０１３６】

B-CASカード６は、第４の実施形態で説明したICカードと異なり、B-CASカード特有の機能（スクランブル処理や受信者確認等）を実現するB-CASカードインタフェース９１と、B-CAS処理部９２とを有する。

【０１３７】

短距離IDの登録処理手順や登録のシーケンス、内部の動作等は第3、第4の実施形態と同様である。

【０１３８】

このように、第３～第５の実施形態では、短距離無線装置４が送信装置２と受信装置３の双方に短距離IDを登録した場合のみ、送信装置２から受信装置３にAVデータを送信できるようにしたため、特定の送信装置２及び受信装置３の間でのみ、AVデータの伝送を許容することができ、AVデータの著作権保護を確実に図ることができる。

【０１３９】

また、短距離無線装置４から送信装置２（または受信装置３）に短距離IDを登録可能な回数を制限することにより、短距離無線装置４の不正使用によるAVデータの不正取得を防止できる。

【０１４０】

さらに、送信装置２と受信装置３に短距離IDを登録する時間間隔を所定時間に設定することにより、遠隔地にある送信装置２または受信装置３への短距離IDの登録を禁止できる。

【０１４１】

また、短距離無線装置４から送信装置２（または受信装置３）に短距離IDを送信する際に、ユーザが送信装置２（または受信装置３）に近づいてボタン操作などを行わないと、短距離IDの登録ができないようにすることで、ユーザの近くにある送信装置２（または受信装置３）のみ登録を許可することができる。

【０１４２】

上述した各実施形態では、著作権保護を図る必要のあるAVデータの伝送について説明したが、本発明は、著作権保護を図る必要のある各種のコンテンツ（電子データ）の伝送に適用可能である。

【０１４３】

図２等で説明した送信装置２，２ａ，２ｂ，２ｃ及び受信装置３，３ａ，３ｂ，３ｃの

内部構成は一例であり、上述した送信装置は受信装置３の機能を備えていてもよいし、逆に上述した受信装置は送信装置の機能を備えていてもよい。

【図面の簡単な説明】

【０１４４】

【図１】本発明に係る通信システムの概略構成を示すブロック図。

【図２】送信装置の一実施形態の概略構成を示すブロック図。

【図３】IDリストの一例を示す図。

【図４】本発明に係る受信装置の内部構成を示すブロック図。

【図５】送信装置と受信装置との間で行われる第１の実施形態におけるAVデータの伝送処理手順を示すシーケンス図。

【図６】図５に続くシーケンス図。

【図７】デバイスIDの登録要求と登録応答を行う際に、なりすましを防止する処理手順を示すシーケンス図。

【図８】第２の実施形態におけるAVデータの伝送処理手順を示すシーケンス図。

【図９】本発明に係る通信装置の第３の実施形態の概略構成を示すブロック図。

【図１０】図９の送信装置の一実施形態の概略構成を示すブロック図。

【図１１】受信装置の一実施形態の概略構成を示すブロック図。

【図１２】送信装置や受信装置内の短距離ID管理部のデータ構造を示す図。

【図１３】短距離無線装置を赤外線リモコン装置で実現した場合の内部構成の一例を示すブロック図。

【図１４】短距離無線装置を無線タグ装置で実現した場合の内部構成の一例を示すブロック図。

【図１５】送信装置及び受信装置における短距離IDの登録処理手順を示すシーケンス図。

【図１６】認証鍵交換および登録用短距離ID送信処理のシーケンス図。

【図１７】送信装置と受信装置との間でAVデータの伝送を行う際の処理手順を示すシーケンス図。

【図１８】上述したステップＳ９１で受信装置から送信された短距離ID＝AAが送信装置の短距離ID管理部に登録されていなかった場合の処理手順を示すシーケンス図。

【図１９】送信装置と受信装置との間でAVデータの伝送を行う際の処理手順を示す別例のシーケンス図。

【図２０】本発明に係る通信装置の第４の実施形態の概略構成を示すブロック図。

【図２１】図２０の送信装置の内部構成の一例を示すブロック図。

【図２２】図２０の受信装置の内部構成の一例を示すブロック図。

【図２３】ICカードの内部構成の一例を示すブロック図。

【図２４】本発明に係る通信システムの第５の実施形態の概略構成を示すブロック図。

【図２５】図２４の受信装置の内部構成の一例を示すブロック図。

【図２６】B-CASカードの内部構成の一例を示すブロック図。

【符号の説明】

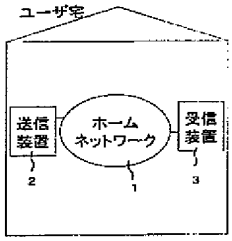
【０１４５】

１　ホームネットワーク
２　送信装置
３　受信装置
１１　ネットワークインタフェース部
１２　通信処理部
１３　DTCPデバイスID記録部
１４　ID管理部
１５　事前登録処理部
１６　時計
１７　認証・鍵交換処理部
１８　暗号処理部

１９　パケット処理部
２０　コンテンツ供給部
２１　ネットワークインタフェース部
２２　通信処理部
２３　DTCPデバイスID記録部
２４　ID管理部
２５　事前登録処理部
２６　時計
２７　認証・鍵交換処理部
２８　暗号処理部
２９　パケット処理部
３０　コンテンツ処理部
４１　短距離無線インタフェース部
４２　短距離無線認証・鍵交換処理部
４３　短距離ID管理部
４４　事前登録処理部
４３ａ，４４ａ　暗号通信処理部
４５　登録終了通知処理部
５１　短距離無線インタフェース部
５２　短距離無線認証・鍵交換処理部
５３　短距離ID管理部
５４　事前登録処理部
５３ａ，５４ａ　暗号通信処理部
５５　登録終了通知処理部
６１　赤外線通信インタフェース部
６２　AV機器初期化処理部
６３　AV機器制御処理部
６４　短距離ID記録部
６５　事前登録処理部
６６　登録回数カウンタ
６７　短距離無線認証・鍵交換処理部
６８　ユーザインタフェース部
６９　時計
７０　無線タグ通信インタフェース部
７１　AV機器初期化処理部
７２　短距離無線認証・鍵交換処理部
７３　事前登録処理部
７４　登録回数カウンタ
７５　短距離ID記録部
７６　ユーザインタフェース部
７７　時計

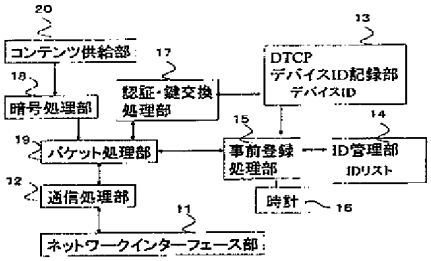
【図１】

第1の実施形態の概略構成



【図２】

送信装置の内部構成



【図３】

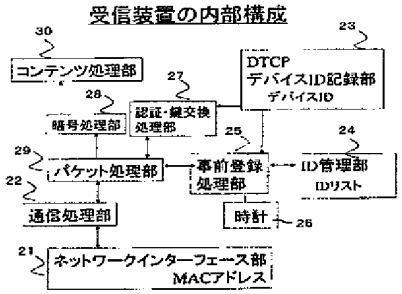
iD管理部内のデバイスIDリスト

必須項目	オプション項目		
対向機器1 デバイスID AA	RTT OOms	固有ID XXX	最終利用日時 △月×日○時×分
対向機器2 デバイスID AA	△△ms	YYY	×月□日△時○分
対向機器3 デバイスID BB	××ms	ZZZ	△月×日○時□分
…	…		

リストは、N個までのデバイスIDの記録が可能。N+1個目の対向機器から登録要求があった場合には、最近使っていない機器、あるいは、FIFO形式で最初に登録した機器を削除して、新規対向機器を登録する

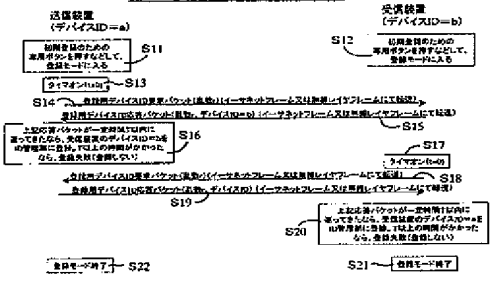
【図４】

受信装置の内部構成



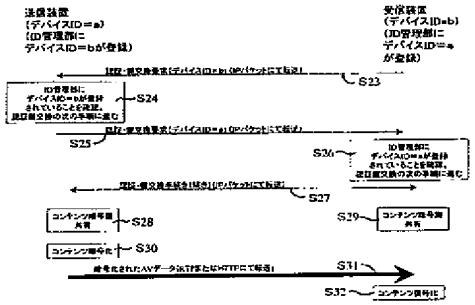
【図５】

第1の実施形態のAV伝送手順



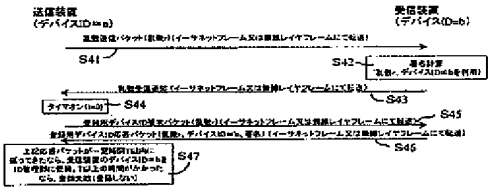
【図６】

第1の実施形態のAV伝送手順



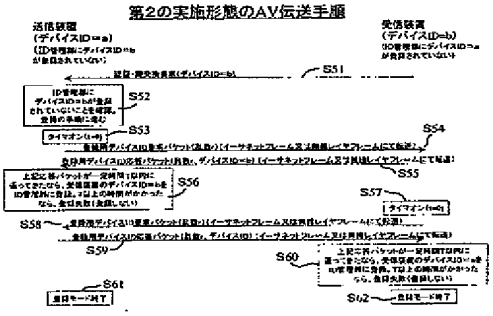
【図７】

なりすまし防止

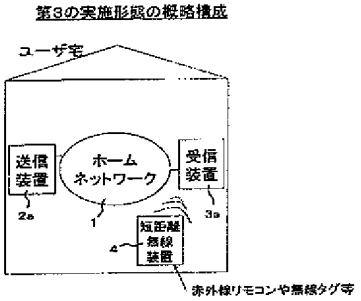


【図８】

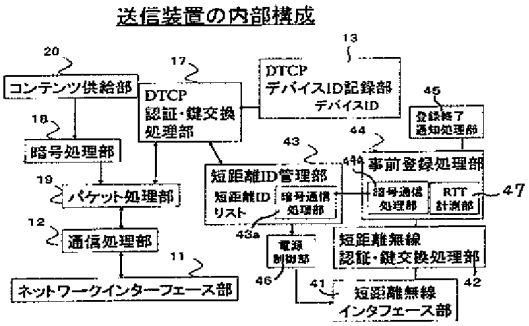
第2の実施形態のAV伝送手順



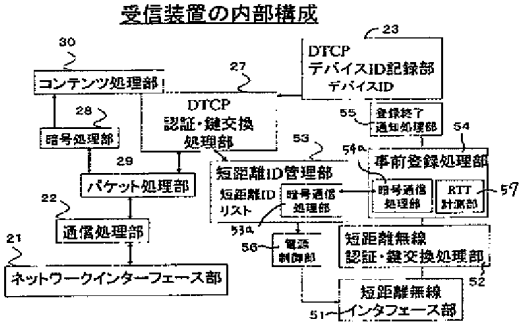
【図９】



【図１０】



【図１１】



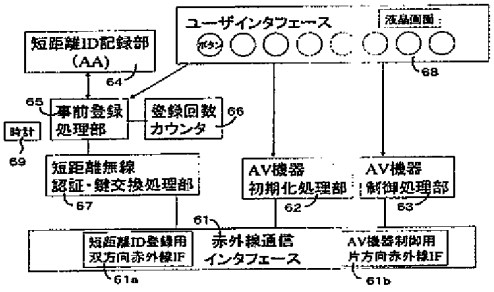
【図１２】

短距離ID管理部内の短距離IDリスト

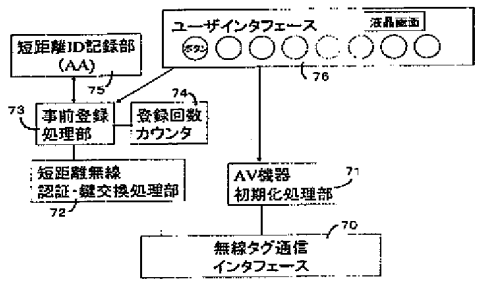
必須項目	オプション項目		
	RTT	DTCPデバイスID	登録日時
(1) 短距離ID＝AA	○○ms	XXX	△月×日○時×分
(2) 短距離ID＝BB	△△ms	YYY	×月□日△時○分
(3) 短距離ID＝CC	××ms	ZZZ	△月×日○時□分
...			

リストは、N個までの短距離IDの記録が可能。N＋1個目の登録要求があった場合には、最近使っていない短距離ID、あるいは、FIFO形式で最初に登録した短距離IDを削除して、新規短距離IDを登録する

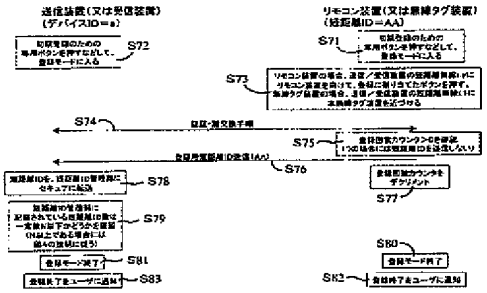
【図１３】



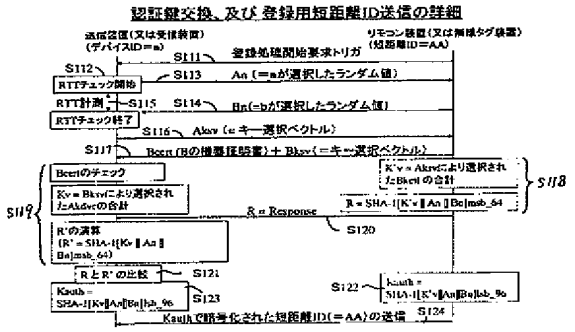
【図１４】



【図１５】

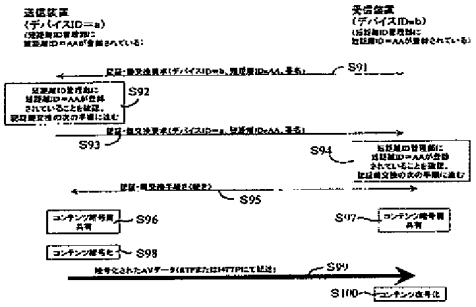


【図１６】



【図１７】

DTCP通信シーケンス

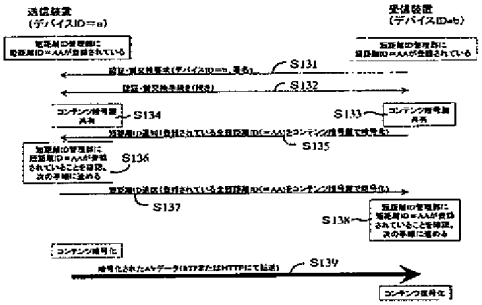


【図１８】

DTCP通信シーケンスの別例

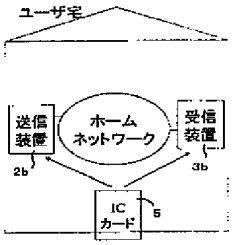
【図１９】

DTCP通信シーケンスの別例



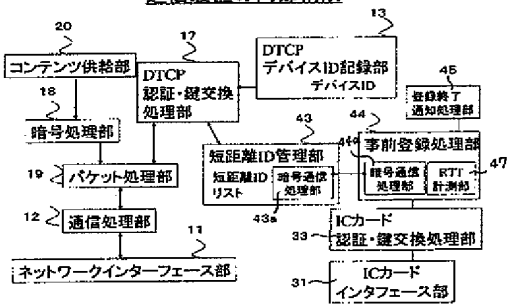
【図２０】

第4の実施形態の全体構成



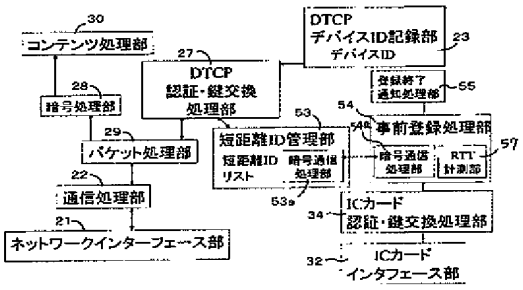
【図２１】

送信装置の内部構成



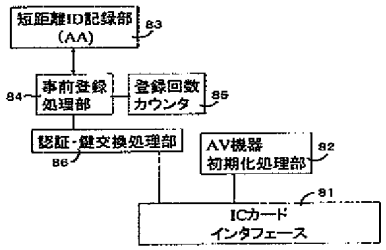
【図２２】

受信装置の内部構成



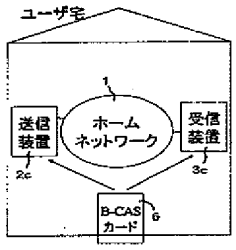
【図２３】

ICカードの内部構成



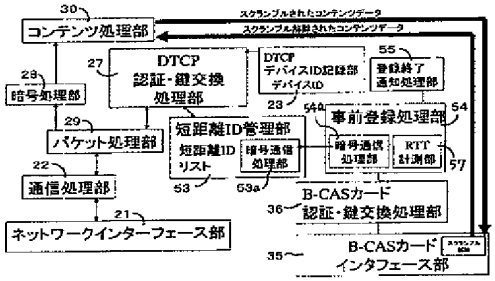
【図２４】

第5の実施形態の全体構成



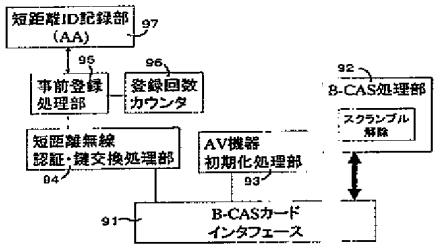
【図２５】

受信装置の内部構成



【図２６】

B-CASカードの内部構成



フロントページの続き

(51) Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	G11B 20/10	H	
	H04L 9/00	675A	

(72)発明者 斉藤 健
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 磯崎 宏
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 松下 達之
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内
(72)発明者 加藤 拓
東京都府中市東芝町１番地 株式会社東芝府中事業所内
(72)発明者 上林 達
神奈川県川崎市幸区小向東芝町１番地 株式会社東芝研究開発センター内

Fターム(参考) 5B017 AA06 CA16
5B085 AA08 AE29 BA06 BG02 BG04 BG07
5D044 AB07 BC01 BC04 BC05 CC01 CC04 CC08 DE49 GK12 GK17
HH15 HL08 HL11
5J104 AA03 AA07 AA12 AA16 EA04 EA18 JA03 KA02 KA04 KA06
NA02 NA05 NA37 NA38 PA07